TÜV Serviceportal

gültig für: Onlinebanking

Prüfgrundlagen

Grundlagen der Zertifizierung

- Der Dienstleistungsprozess ist angemessen dokumentiert. Die wesentlichen Dokumentationen sind verfügbar und bekanntgemacht. Die Anforderungen neuer Entwicklungen oder erheblicher Änderungen am Portal werden ausreichend dokumentiert. Ein Freigabeprozess ist installiert und umgesetzt.
- Die Kommunikationsmittel für die Dienstleistung sind vollständig. Sie enthalten für den User verständliche Informationen. Dies gilt für alle dargestellten Informationen auf der Website, Werbemittel (wie Flyer, Prospekte, Anzeigen), Allgemeine Geschäftsbedingungen oder Nutzungsbedingungen und andere Kommunikationsmittel. Ein Aktualisierungsprozess für die Informationen ist installiert und umgesetzt.
- Der Dienstleistungsprozess ist im Unternehmen umgesetzt. Es sind geeignete Verfahren wirksam, die die Kriterien in der Organisation umsetzen. Die fortlaufende Aktualisierung ist sichergestellt. Entwicklung und Dokumentation folgen geregelten Prozessen. Der Betreiber stellt durch geeignete Maßnahmen sicher, dass Prozesse und Richtlinien eingehalten werden.
- Das Management kontrolliert den Dienstleistungsprozess. Aus der regelmäßigen Ermittlung der Bedürfnisse der beteiligten Parteien werden Maßnahmen und Ziele abgeleitet. Die Wirksamkeit der Maßnahmen und Ziele wird überprüft. Die Existenz ausreichender Ressourcen und Verantwortlichkeiten wird ebenfalls überprüft. Für Entwicklungen und Änderungen ist sichergestellt, dass eine angemessene Qualitätssicherung befolgt wird und ausgewählte Mindestanforderungen erfüllt werden. Ein Prozess zur Prüfung und Freigabe neuer Funktionen und Entwicklungen ist definiert und wirksam umgesetzt.

Funktionen und Anwendungen des Portals

- Die Voraussetzung für eine Online-Kontoeröffnung werden bereits zu Beginn der Antragstellung verständlich und vollständig kommuniziert. Ebenso wird das Legitimationsverfahren genannt.
- Die Legitimation zur Kontoeröffnung kann in einer Filiale vor Ort erfolgen. Fern-Legitimationen können ebenfalls angeboten werden. Werden Fern-Legitimationen angeboten, so wird mindestens ein als sehr sicher eingestuftes Verfahren (Post-Ident-Verfahren oder Belegverfahren (pdf-Formulare) angewendet.
- Kann die Legitimation auch per Video-Ident-Verfahren erfolgen, so werden mindestens die aktuellen Anforderungen an die Nutzung von Videoidentifizierungsverfahren der Bafin erfüllt.
- Es werden mindestens zwei unterschiedliche Kanäle für das Onlinebanking-Verfahren angeboten. Neben dem Verfahren über Internetbrowser oder Mobile Banking wird auch das HBCI- bzw. FinTS-Verfahren angeboten.
- Die Kunden erhalten aktiv Hinweise auf Verwendung einer HBCI-bzw. FinTS-Finanzsoftware. Diese werden als sehr sichereingestuft.

- Neben den Standardanmeldeanforderungen (Nutzerkennung mit Passwort) wird auch die sogenannte Zwei-Faktor-Authentisierung (2FA) angeboten. Transaktionen können nur mit einer zusätzlichen Sicherheitsverfahren durchgeführt werden.
- Für den Zugang zum Online-Konto sind Passwortrichtlinien nach dem Stand der Technik einzuhalten. Dem Nutzer müssen geeignete und sichere Verfahren zum Ändern von Passwörtern bereitgestellt werden. Es wird ein sicheres Verfahren zum Anfordern vergessener Passwörter angeboten.
- Wird das Passwort bzw. PIN dreimal falsch eingeben, wird der Online-Banking Zugang aus Sicherheitsgründen automatisch gesperrt. Die Sperrung bezieht sich ausschließlich auf die Online-Banking-Anwendung.
- Es steht ein gesichertes Verfahren Entsperrung des Zugangs zur Verfügung.
- Der Kunde hat eine ausreichende Auswahl an Mittel der Authentifizierung für Transaktionen. Neben den Verfahren, die derzeit mit hoher Sicherheit eingestuft werden (Best-Sign mit Smartphone, Photo-Tan mit Smartphone, App-Tan und SMS-Tan), steht auch mindestens ein Verfahren mit sehr hoher Sicherheit (ChipTan, (Best-Sign mit Lesegerät, PhotoTan mit Lesegerät und QR-Tan) zur Verfügung.
- Die Kunden haben die Möglichkeit, Limits für Überweisungen selbst festzulegen.
- Es steht ein Prozess innerhalb des Onlinebanking für die Aktivierung neuer Handy-Nummern für mobile TANs zur Verfügung.

Datensicherheit und Datenschutz

- Dem Nutzer werden Hinweise und Informationen zum Umgang mit schützenswerten Daten gegeben. Die Hinweise und Informationen sind umfangreich und im System einfach auffindbar.
- Die Nutzung von Tracking-Diensten ist nur nach (vorheriger) Einwilligung des Betroffenen zulässig. Wenn Tracking-, Analyse- und Statistikdienste eingesetzt werden, die personenbezogene Daten erheben, verarbeiten oder nutzen, muss der Betreiber eine entsprechende Information in den Datenschutzhinweisen hinterlegen und gesondert die Einwilligung zur Nutzung dieser Dienste einholen.
- Ein Datenschutzbeauftragter ist schriftlich bestellt. Zur Erfüllung seiner Aufgaben hat er die erforderliche Fachkunde und Zuverlässigkeit. Dieser ist der Geschäftsführung direkt unterstellt und in der Ausübung seiner Tätigkeit weisungsfrei.
- Für den Fall einer risikobehafteten Verletzung des Schutzes personenbezogener Daten hat der Diensteanbieter einen effektiven Prozess zur Meldung gegenüber der zuständigen Aufsichtsbehörde etabliert.
- Die DSGVO schützt die betroffenen Personen und sieht deshalb Rechte Betroffener vor, die einen Anspruch gegenüber dem Unternehmen begründen. Das Unternehmen hat Prozesse etabliert, um Anfragen unverzüglich entsprechen zu können.

Datensicherheit und Datenschutz

- Die eingesetzten Protokolle zur SSL/TLS Verschlüsselung entsprechen dem aktuellen Stand der Technik.
- Cipher-Suites (Chiffrensammlung für den Datenverkehr zwischen einem Server und einem Client) entsprechen dem neuesten Stand der Technik.
- Die eingesetzten Zertifikate sind auf eine vertrauenswürdige Zertifizierungsstelle

zurückzuführen. Mit Hilfe der von der CA ausgestellten digitalen Zertifikate werden Identitäten im Internet überprüft. Die verschlüsselten Verbindungen sind in der Adresszeile des Browsers zu erkennen.

- Durch geeignete Maßnahmen wird sichergestellt, dass die aktiven Sessions dem Stand der Technik entsprechend gesichert sind. Es erfolgt ein Hinweis auf Einsatz von Cookies.

IT-Infrastruktur

- Für betriebsrelevante Systeme ist ein Mindestmaß an Verfügbarkeit, in Einklang mit den vertraglich festgehaltenen Kundenvereinbarungen, sichergestellt. Die Gewährleistung der Verfügbarkeit unterliegt einer fortwährenden Überprüfung. Der Betreiber hat geeignete Maßnahmen zur Systemüberwachung installiert.
- Der Betreiber verfügt über eine umfassende und aktuelle Dokumentation der eingesetzten IT-Systeme.
- Betriebsrelevante Systeme sind physisch ausreichend vor unbefugtem Zugriff geschützt. Geeignete Maßnahmen zum Netzwerkschutz sind vorhanden. Ein ausfallsicherer Betrieb von kritischen Komponenten ist sichergestellt. Das Rechenzentrum entspricht dem Stand der Technik und ist ausreichend physikalisch gesichert.
- Die IT-Infrastruktur wird regelmäßig gewartet und aktualisiert. Der Betreiber hat einen Prozess definiert und wirksam umgesetzt, um kritische Schwachstellen zu identifizieren und unverzüglich zu behandeln.
- Eine geeignete Firewall ist vorhanden und wird aktiv verwaltet.
- Der Betreiber stellt sicher, dass ein geeigneter Virenschutz vorhanden ist und regelmäßig aktualisiert wird.
- Ein Rechte- und Rollenkonzept ist umgesetzt und wird regelmäßig überprüft.
- Es existiert ein wirksames Back- und Restorekonzept. Insbesondere wird bei Systemausfall eine wirksame Widerherstellung der Systeme/Daten gewährleistet.
- Daten mit hohem Schutzbedarf sind mit Methoden nach dem Stand der Technik verschlüsselt.
- Der Betreiber reagiert zeitnah auf aktuelle Sicherheitsbedrohungen.

Layout und Ergonomie

- Die Startseite ist übersichtlich strukturiert. Die Nutzer finden sich auf der Homepage sofort zurecht. Die Navigation ist übersichtlich angeordnet und selbst beschreibend.
- Wichtige Informationsseiten (Anbieterkennung, Datenschutz, AGB, etc.) sind von der Startseite leicht erreichbar.
- Die Schriftart unterstützt das Lesen der Texte. Die Farbkombinationen weisen ausreichende Kontraste auf. Sie erleichtern das Lesen der Informationstexte.
- Die Navigation ist übersichtlich angeordnet und selbst beschreibend.
- Der Webauftritt hat eine Sitemap-Funktion (Seitenübersicht).
- Das Portal verfügt über eine benutzerfreundliche und unterstützende Suchfunktion.
- Das System muss für den Nutzer effektiv und effizient nutzbar sein und den Nutzer bei der Erledigung seiner Aufgaben unterstützen. Die Menge der dargestellten Informationen darf den Nutzer nicht behindern.
- Das System bietet dem Nutzer in geeigneter Weise allgemeine und zielgerichtete Hilfestellungen

sowie bei Eingaben und Anfragen über den Bearbeitungsstand / Status passende Informationen. Das Portal muss den Nutzer beim Erlernen der Bedienung angemessen unterstützen und eine entsprechende Einführung / Anleitung bereitstellen. Sind Eingaben erforderlich, müssen geeignete Rückmeldungen vorgesehen sein, insbesondere auch dann, wenn fehlerhafte Eingaben dazu führen, dass ein Vorgang nicht ausgeführt werden kann.

- Das System ist vom Nutzer steuerbar und richtet sich bei der Bedienung nach der Arbeitsgeschwindigkeit des Nutzers.
- Unbeabsichtigte formative Fehleingaben durch den Nutzer führen nicht zu Systemabstürzen oder undefinierten Systemzuständen. Das System erkennt formative Fehleingaben des Nutzers. Es werden sinnvolle Korrekturhinweise gegeben.
- Das System ist in Darstellung und Sprache auf die Bedürfnisse des Nutzers anpassbar. Die ursprüngliche Ansicht ist nach Veränderungen durch den Nutzer wiederherstellbar. Die Darstellung und Funktionalität ist für verschiedene Geräteklassen und Browser gewährleistet und ist dabei nicht wesentlich unterschiedlich oder funktional eingeschränkt.

Verständlichkeit

- Das Portal erlaubt dem Nutzer eine einfache selbsterklärende Anwendung. Die Darstellung der angebotenen Informationen ist übersichtlich und umfassend. Die Texte sind verständlich.
- Die sprachliche Gestaltung geschieht in einer dem Inhalt und der Zielgruppe angemessenen, einfachen und verständlichen Form. Wo erforderlich, werden dem Nutzer sinnvolle Rückmeldungen gegeben.
- Der Text der Allgemeine Geschäftsbedingungen (AGB) oder Nutzungsbedingungen (NB) ist aufrufbar. Er ist für den Nutzer sind einfach lesbar und verständlich formuliert.
- Werbung (Fremdwerbung) ist von Angebot / Information deutlich erkennbar abgegrenzt.

Allgemeine Informationspflichten

- Das Portal vermittelt eine ausreichende Transparenz. Die Identität des Betreibers ist eindeutig dargelegt. Die umfassende Information zum Betreiber ist einfach und schnell zu finden (one click away).
- Das Portal hat eine Anbieterkennzeichnung. Es ist z.B. ein Impressum mit den erforderlichen Angaben vorhanden. Die Angaben sind schnell erreichbar. Der Inhalt ist korrekt. Die Aussagen sind zutreffend und ständig verfügbar.
- Allgemeine Geschäftsbedingungen (AGB) oder Nutzungsbedingungen (NB) sind aufrufbar. Diese sind leicht auffindbar (one click away). Die notwendige Nachvollziehbarkeit (Klarheit) ist gegeben. Werbeaussagen stehen im Einklang mit den AGB / NB. Die AGB bzw. NB sind einfach lesbar und verständlich (Hohenheimer-Index mind. 6).
- Die AGB- / NB-Zustimmung ist eindeutig.
- Es besteht eine elektronische Kontaktmöglichkeit.
- Zur Beilegung von Streitigkeiten ist ein Link zur OS-Plattform vorhanden. Die Europäische Kommission stellt unter http://ec.europa.eu/consumers/odr/ eine Plattform zur außergerichtlichen Online-Streitbeilegung (sogenannte OS-Plattform) bereit.

Serviceleistungen

- Es werden mehrere Kanäle für die Erreichbarkeit des Kundenservice angeboten. Der Kundenservice ist mindestens telefonisch oder per Email erreichbar.
- Für die telefonische Erreichbarkeit werden auch Zeiten außerhalb der Filialöffnungszeiten angeboten. Werktäglich stehen mindestens 10 Stunden Erreichbarkeit zur Verfügung.
- Das eingesetzte Personal hat die notwendigen Fach- und Spezialkenntnisse zur Bewertung der Informationen.
- Mobile TANs (pro SMS) werden kostenfrei versendet.
- Sofern TAN-Generatoren angeboten werden, wird mindestens ein Gerät angeboten, dessen Kosten 20 € nicht übersteigen. Außerdem wird auch ein Gerät mit Multibankenfähigkeit angeboten.
- Der Betreiber klärt den Nutzer ausführlich über die Möglichkeiten zum Schutz vor Missbrauch auf. Die Aufklärung enthält auch Hinweise für den Schutz der vom Kunden genutzten Hard- und Software. Die Hinweise entsprechen mindestens den Informationen des Bundesamtes für Sicherheit in der Informationstechnologie (Checkliste Onlinebanking).
- Es ist eine gesonderte Kontaktadresse für Missbrauchs-Meldungen vorhanden.
- Die Kunden erhalten Hinweise auf Finanzsoftware-Programme. Es kann mindestens ein Finanzsoftware-Programm vergünstigt vermittelt werden. Die Kunden können Online-Anleitungen für die Finanzsoftware kostenlos downloaden oder ein Download-Link für den kostenlosen Download wird zur Verfügung gestellt.
- Für die Bearbeitung von Rückmeldungen / Beschwerden der Nutzer muss der Anbieter einen angemessenen und wirkungsvollen Prozess beschrieben haben und diesen effektiv anwenden.
- Der Betreiber bietet Hinweise auf Sicherheitsvorkehrungen außerhalb der Website an.
- Ein Informationssystem über aktuelle Sicherheitsthemen steht zur Verfügung gestellt. Die Informationen sind verständlich und klar aufbereitet. Die Aktualität ist gewährleistet.
- Ein Informationssystem mit Hinweisen über aktuelle Betrugsmaschen und Gefahren ist eingerichtet.